NORTH DAKOTA

HOMELAND SECURITY

ANIT-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Regional

National

International

Banking and Finance Industry

Chemical and Hazardous Materials Sector

Commercial Facilities

Communications Sector

Critical Manufacturing

Defense Industrial Base Sector

Emergency Services

Energy

Food and Agriculture

Government Sector (including Schools and Universities)

Information Technology and Telecommunications

National Monuments and Icons

Postal and Shipping

Public Health

Transportation

Water and Dams

North Dakota Homeland Security Contacts

North Dakota

Defendants agree to plea deal in N.D. bank fraud case. A former North Dakota bank vice president and her husband signed plea agreements in a scheme to bilk hundreds of thousands of dollars from trust accounts, the Associated Press reported May 1. Court documents accused the former vice president of defrauding Bank of the West customers out of nearly $800,000 while she was working as a trust officer. The woman and her husband are facing federal charges of conspiracy to commit bank fraud. The plea agreement in the criminal case calls for Bank of the West to be paid back $790,893. The fraud dates back to 2001, according to court documents. Source: http://www.jamestownsun.com/event/article/id/159975/group/News

Regional

(Minnesota) **Cell tower outage affecting Sprint customers.** Sprint customers trying to use their cell phones in parts of Waite Park and west St. Cloud, Minnesota, found themselves still without service May 1. Sprint officials said they experienced a cell site outage in west St. Cloud since April 29. A Waite Park Sprint store manager said a cell site team was on site working to restore service. She said a T-1 circuit was malfunctioning at the site. There was no time estimate for repairs as of May 1. Source: http://wjon.com/cell-tower-outage-affecting-sprint-customers/

(South Dakota) **Minnow discovery will delay repairs to SD dam.** The planned rebuilding of the Rosehill dam in Hand County, South Dakota will be delayed by the discovery of an endangered minnow. The dam failed in July 2010 during heavy rains. The endangered Topeka shiner minnow was recently discovered in Sand Creek, near the dam. The minnow's presence means South Dakota's Game, Fish, and Parks Department has to consult federal agencies to make sure the dam project does not affect the population. The regional South Dakota agency manager said the dam's reconstruction will probably be delayed until the fall of 2013. Source: http://www.thenorthwestern.com/usatoday/article/39166023?odyssey=mod|newswell|text|FRONTPAGE|p

National

Nothing Significant to Report

International

UK arrests 7 on suspicion of funding terror. Seven people were arrested in Great Britain on suspicion of financing terrorism in Somalia by smuggling a leaf that can produce a mild high into the United States, officials said May 1. Scotland Yard said the group was arrested as part of an operation that involved Homeland Security Investigations, the investigative branch of U.S. Immigrations and Customs Enforcement (ICE). It investigated a network suspected of illegally exporting a leaf known as khat from the United Kingdom, where it is legal, to the United States and Canada, where it is a controlled substance, Scotland Yard said. "The proceeds generated by

this illegal activity (were) then transferred back to Somalia," a spokesman for ICE said. He added that the khat mostly originated from Kenya, and U.S. law enforcement officials were working closely with their counterparts overseas on the investigation. British police said one woman and six men were arrested May 1 at four separate residences in London, Coventry, and Cardiff, Wales. Those four homes are being searched along with seven other residential addresses and a business address in Coventry, police added. Police said the seven people arrested are suspected of involvement in funding a terrorist organization and laundering the proceeds of crime for that purpose. Source: http://www.google.com/hostednews/ap/article/ALeqM5iSKIv2aF2FA-IHAaZKwvbATi9TRQ?docId=af3bf8ee287e4036aed4e593ddf8f2ec

New foot-and-mouth disease strain spreads from N. Africa: UN. The Food and Agriculture Organization (FAO) in Rome, Italy, said an outbreak of the SAT2 strain of foot-and-mouth disease (FMD) was found in Rafah in the southern part of Gaza Strip on the border with Egypt. The FAO was sending 20,000 vaccine doses immediately, Agence France-Presse reported May 2. "If FMD SAT2 reaches deeper into the Middle East it could spread throughout vast areas, threatening the Gulf countries — even southern and eastern Europe, and perhaps beyond," said the FAO's chief veterinary officer. He said vaccines against the SAT2 virus were in short supply. He also said the immediate priority should be to limit the movement of animals to prevent the highly infectious disease from spreading further. The agency said it would send an extra 40,000 vaccine doses to Gaza as soon as possible. It said Israel already implemented a targeted vaccination program. Source: http://medicalxpress.com/news/2012-05-foot-and-mouth-disease-strain-africa.html

North Korea jamming' hits South Korea flights. Jamming signals thought to be from North Korea have affected GPS navigation on at least 250 flights, BBC News reported May 2. Nine South Korean and nine foreign airlines were affected since April 28, the South Korean Transport Ministry said. The flights had to rely on alternative navigation systems but were in no danger, the ministry added. The south has accused the north — with which it remains technically at war — of similar incidents in the past. "We've confirmed the GPS jamming signals have been stemming from the north," the deputy director at Seoul's Korea Communications Commission said. He said there was "no serious threat to the safety of flights because planes are using other navigation devices". Source: http://www.bbc.co.uk/news/world-asia-17922021

Aerial Greenpeace protester strikes at French nuclear site, dropping smoke bomb on reactor. An environmental activist was arrested May 2 after dropping a billowing smoke bomb onto the roof of a French nuclear reactor ahead of a key presidential election debate, Greenpeace and French police said. Video footage from the stunt captured the airborne activist on a motorized paraglider after he dropped the smoke bomb at the Bugey site east of Lyon. The man was arrested after descending to the ground. A Greenpeace nuclear spokesman said that the spectacle was meant to stimulate a political debate on nuclear power. Source: http://www.washingtonpost.com/business/aerial-greenpeace-protestor-strikes-at-french-nuclear-site-dropping-smoke-bomb-on-reactor/2012/05/02/gIQA3hj4vT_story.html

Phishing email targets Santander clients. Customers of Santander, one of the largest banking groups in the world, are currently being targeted with a phishing e-mail masquerading as a bogus notification of a scheduled software upgrade. According to Hoax-Slayer, the offered link takes users to a spoofed Santander online banking Web site, where they are asked to enter their ID, passcode, customer PIN, mobile number, landline number, and date of birth. Having done that, the site requests users to set up three security questions and answers, which are then misused by the phishers to gain access to the users' account. In the end, users are redirected to the legitimate Web site of Santander's United Kingdom branch in order to maintain the illusion that nothing out of the ordinary happened. Source: http://www.net-security.org/secworld.php?id=12834

Banking and Finance Industry

New email claims to be from FDIC, threatens users confidential and personal data. A fraudulent e-mail offering cash in return for survey information could obtain access to personal and confidential data, WEWS 5 Cleveland reported April 27. The Federal Deposit Insurance Corporation (FDIC) issued a warning to computer users that it received numerous reports of fraudulent e-mails that have the appearance of having been sent by the FDIC. The e-mail contains a subject line "Survey Code: STJSPNUPUT." It reads "you have been chosen by the FDIC to take part in our quick and easy 5 question survey. In response, will credit $100 dollars to your account just for your time." The FDIC is warning consumers not to click on the link provided in the e-mail, as it is intended to obtain personal information or load malicious software onto users' computers. The FDIC reminds consumers that it does not send unsolicited e-mail to consumers or business account holders. Source: http://www.newsnet5.com/dpp/news/local_news/investigations/new-email-claims-to-be-from-fdic-threatens-users-confidential-and-personal-data

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(Pennsylvania) **Man seals off hotel room, mixes chemicals to commit suicide.** Police in Swatara, Pennsylvania, were called to a Super 8 motel on the report of a suspicious odor, May 3, and discovered a room sealed shut with duct tape. When officers were unable to contact the occupant, they feared toxic materials were used in the room. Officers evacuated the motel and requested fire, EMS, and HAZMAT crews. After entering the room, officers discovered the room's occupant had mixed several chemicals to create toxic fumes to commit suicide. The man did not survive. The scene was decontaminated, as were members of the responding agencies. Source: http://www.whptv.com/news/local/story/Man-seals-off-hotel-room-mixes-chemicals-to/oIpnx8LYpEC6nRaVIFcrIQ.cspx

(Missouri) **St. Louis tent collapse raises safety questions.** St. Louis officials are expected to more closely scrutinize the large tents commonly set up near downtown stadiums after one of the temporary structures collapsed in high winds April 28, resulting in the death of an Illinois man and dozens of injuries after a baseball game. A spokesman for the city's mayor said it was unclear if adequate regulations were in place and being followed or if the disaster was simply the result of people not paying attention to severe weather warnings. The fast-moving storm ripped a large beer tent at Kilroy's Sports Bar from its moorings and sent it and debris hurtling through the air about 80 minutes after the end of a St. Louis Cardinals Major League Baseball game. Seventeen people in the tent were taken to hospitals, and up to 100 of the 200 gathered were treated at the scene, which was near Busch Stadium. Source: http://www.weather.com/outlook/weather-news/news/articles/st-louis-tent-collapse_2012-04-28

Communications Sector

(Hawaii) **Copper thefts leave H3 call boxes inoperable.** The Hawaii State Department of Transportation (DOT) is seeking the public's help in stopping new thefts of copper wiring on the H-3 Freeway, Maui Now reported May 1. DOT officials said electrical copper wiring on the H-3 Freeway was cut sometime in late April. The incident was reported on the Halawa-side of the tunnels, near the Halawa Interchange. As a result, the damage rendered all emergency call boxes and six traffic monitoring cameras on the Halawa-side of the tunnels inoperable. Fiber optic communications cabling was also cut, affecting control over electronic message boards that are used to display tunnel lane closure information on the Halawa-side. The copper wiring in several conduits was also cut, but not taken. Police reports were filed and repairs to the wiring are pending. Source: http://mauinow.com/2012/05/01/copper-thefts-leave-h3-call-boxes-inoperable/

(Ohio) **Thieves disrupt telephone and Internet service to hundreds in Warren today.** The theft of 2 60-foot cables strung on utility poles disrupted telephone and Internet service to up to 500 businesses and residents in the northwest quadrant of Warren, Ohio, for much of April 27. A Century Link representative contacted the Warren Police Department about the theft, saying it occurred sometime overnight. The cost to replace the cables, which were 1.5- to 2-inches in diameter will be about $10,000, officials estimated. Because of the cost of the cable, the theft was entered into the report as felony theft, and because of the effect on customers, it was also entered in as a disruption of public services. Source: http://www.vindy.com/news/2012/apr/27/thieves-disrupt-telephone-and-internet-service-hun/?nw

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

Feds: Soldier sold stolen arms on eBay. A U.S. soldier with connections to Orlando, Florida, sold stolen arms to buyers on eBay while he was deployed in Iraq in 2010, according to DHS investigators. The man is accused of violating federal law regarding the export of sensitive technology such as night-vision equipment, rifle scopes, and high-powered infrared lasers not intended for the public, according to an affidavit filed in federal court in Orlando. The man told buyers he was retired from the military and based in Orlando selling surplus equipment, investigators said. His listing touted the arms as being extremely rare and "impossible to find on the international market," the affidavit said. He shipped lasers to buyers in Japan and Nevada, a high-tech satellite phone was sent to Kuwait, and other equipment was shipped to California. The items were sold for a few thousand dollars each. eBay eventually took down the postings because they violated its policies. Investigators tracked down some recipients and recovered stolen items. The man told investigators that while he was in the military guarding non-combat envoys, he came across a container with the items and brought them all back to Orlando. He claimed he did not know civilians were prohibited from possessing the equipment, but knew it was wrong to sell them. However, the man's e-mails with a buyer in Japan show he knew he was violating international arms trafficking regulations and falsified shipping documents to conceal the items as "auto parts." Source: http://www.military.com/news/article/feds-soldier-sold-stolen-arms-on-ebay.html

Emergency Services

(West Virginia) **Two men face charges in theft of copper from police phone lines.** State police troopers arrested two men May 1 who allegedly stole copper from a State police detachment in Boone County, West Virginia. A State police sergeant said troopers began investigating a copper theft from phone lines at the StatepPolice detachment in Whitesville. The investigation led troopers to the two suspects, he said. Police charged the men with interruption of telephone service, grand larceny, and conspiracy to commit a felony. The theft caused about $25,000 in damage and disrupted phone service for the detachment and community for nearly 2 days, the sergeant said. Source: http://sundaygazettemail.com/News/201205030129

Tasers can be tied to cardiac arrest and death, new study finds. A new study published the week of April 30 in the journal Circulation finds the use of Tasers can be tied to cardiac arrest and death. The study represents the first peer-reviewed evidence that Tasers can bear a lethal risk. An electrophysiologist at Indiana University wrote that a review of "animal and clinical data" showed that Taser strikes to the chest can "cause cardiac electrical capture," which can trigger a heart attack. The Taser, used by about 16,000 law enforcement agencies around the world, is marketed as a way to subdue an individual without causing substantial injury or death, but since 2001, more than 500 people have died following Taser stuns, according to Amnesty International, which said in February that stricter guidelines for its use were "imperative." Although, in only a few dozen of those cases have medical examiners ruled the Taser contributed to the death. And TASER International, the company who makes the weapon, cited a U.S. Department of Justice study in May that concluded "there is currently no medical

evidence that CEDs (controlled energy devices, which include Tasers) pose a significant risk." The Justice study also reported that "the risks of cardiac arrhythmias or death remain low and make CEDs more favorable than other weapons." Source: http://www.therepublic.com/view/story/tasers-heart/tasers-heart/

(Wisconsin) **Police used excessive force with rubber bullets, court rules.** A federal appeals court found Waukesha, Wisconsin police used excessive force when they shot a suspected drunken driver four times with rubber bullets in 2005, the Milwaukee Journal Sentinel reported April 30. One of the shots caused a 6-inch gash in the driver's ankle that required 30 stitches. The 7th U.S. Circuit Court of Appeals ruled in a 2-1 decision that a trial judge should have granted the victim motion for judgment as a matter of law, despite a jury's verdict in favor of the police. The case now heads back to federal district court in Milwaukee for a hearing on the extent of the driver's damages and attorney fees. Source: http://www.jsonline.com/news/waukesha/waukesha-police-used-excessive-force-with-rubber-bullets-court-rules-cc57pue-149604155.html

(Florida) **AntiSec hackers steal 40 GB of data from Lake County Sheriff's Office.** Softpedia reported April 28 a massive 40 gigabytes worth of files were stolen by Anonymous hackers operating under the AntiSec banner from the internal networks of the Lake County Sheriff's Office (LCSO) in Florida. One of the hackers that participated in the operation told Softpedia that out of the 40 gigabytes of data, around 35 gigabytes represent forensic software and other applications used by law enforcement agencies. The other 5 gigabytes are made up of reports that detail LCSO operations such as Op Inmate Intelligence Gathering and Operation Screen Savers. The files also include corporate security IPDR reports from Sprint Nextel that show the telecoms firm hands over private data to the authorities. Phone lists that reveal financial crimes, intelligence bulletins from the FBI, communication codes, and communications equipment are all contained in the data dump. Furthermore, hackers leaked the locations of U.S. Army Reserve facilities, badge numbers, 9-1-1 calls, log-in credentials, manuals, and official bulletins from the Department of Justice. Source: http://news.softpedia.com/news/AntiSec-Hackers-Leak-40-GB-of-Data-from-Lake-County-Sheriff-s-Office-266784.shtml

(Texas) **No water found in hydrants during apartment fire.** When firefighters responded to a fire April 29 that eventually destroyed 8 apartments and displaced 18 people in San Antonio, the firefighters were forced to search beyond nearby hydrants as two of the first hydrants were dry. The fire department plans to get to the bottom of why the hydrants were dry. They will look into who is in charge of the hydrants: the city or a private owner. If it is the city the fire department runs inspections and the San Antonio Water System makes repairs. Hydrant inspections happen about once a year. Source: http://www.woai.com/mostpopular/story/No-water-found-in-hydrants-during-apartment-fire/dFxSgcLrxkSGbldqJztE_A.cspx

ENERGY

Interior sets new drilling rules on public land. The U.S. Presidential administration said May 4 it will require companies drillingfor natural gas on public and Indian lands to publicly disclose

chemicals used in hydraulic fracturing operations. The proposed "fracking" rules also set standards for proper construction of wells and wastewater disposal. The Department of Interior secretary said the long-awaited rules will allow continued expansion of natural gas drilling while protecting public health and safety. The government maintains the new rules, which have been under consideration for a year and a half, reflect industry concerns. For instance, the rule on disclosure of chemicals used in fracking was softened to allow companies to file reports after drilling operations are completed, rather than before they begin, as initially proposed. Industry groups said the earlier proposal could have caused lengthy delays. Source: http://www.kgwn.tv/story/18146854/interior-sets-new-drilling-rules

(Pennsylvania) **Copper thieves damage substations.** Met-Ed and police in Pennsylvania were investigating a series of thefts of copper grounding wires and equipment from electric substations. The thefts occurred in West Reading, Muhlenberg Township, Lincoln Park, Leesport, and the Moselem Springs area of Richmond Township, a Met-Ed spokesman said. People climbed safety fences or cut through the fences and damaged the substations, making them unsafe for employees who routinely service the facilities and must repair the damage. "The damage also has resulted in power outages to homes and businesses as recently as [the week of April 23]," he said. The spokesman urged the public to report any suspicious activity. Source: http://readingeagle.com/article.aspx?id=383853

Backdoor that threatens power stations to be purged from control system. Mission-critical routers used to control electric substations and other critical infrastructure are being updated to remove a previously undocumented backdoor that could allow vandals to hijack the devices, manufacturer RuggedCom said April 27. The announcement by the Ontario, Canada-based company comes 2 days after Ars Technica reported the company's entire line of devices running its Rugged Operating System contained a backdoor with an easily determined password. The backdoor, which cannot be disabled, had not been publicly acknowledged by the company until now, leaving the power utilities, military facilities, and municipal traffic departments using the industrial-strength gear vulnerable to sabotage that could affect the safety of huge populations of people. Source: http://arstechnica.com/business/news/2012/04/backdoor-that-threated-power-stations-to-be-purged-from-control-system.ars

Food and Agriculture

PepsiCo recalls Tropicana OJ after 'microbiological contamination' dispatch error. PepsiCo UK initiated a recall of Tropicana Kids Orange Juice Drinks over fears the cartons contain potentially hazardous water rather than the typical orange juice blend, Food Quality News reported May 3. Nearly 300 units of Tropicana Kids Orange Juice Drinks multi-packs were recalled by the firm after it emerged that water in the packs was of an "unsatisfactory quality due to microbiological contamination." In a statement sent to Food Quality News, a PepsiCo spokesperson attributed the error to the accidental dispatch of samples from a production test procedure using water that was not up to the firm's usual standards. Source: http://www.foodqualitynews.com/Food-Alerts/PepsiCo-recalls-Tropicana-OJ-after-microbiological-contamination-dispatch-error

Rare Salmonella Paratyphi outbreak grows as investigation continues. The outbreak of a rare, typhoidal Salmonella strain that originated in North Carolina's Buncombe County grew to 40 confirmed illnesses May 3 as the State and county health departments continued their investigation and anticipate additional infections will surface. According to a Buncombe County Department of Health spokeswoman, many of those sickened contracted their infections through person-to-person contact. April 30, Smiling Hara recalled 12-ounce packages of unpasteurized tempeh as a cautionary measure after a sample of the company's soybean tempeh tested positive for Salmonella. The tempeh remains a potential outbreak source until further tests. More than half of the cases involve individuals who said they did not consume tempeh during the outbreak window, the health spokeswoman said. The health departments continue to investigate other potential sources, she said, though it is clear that infections have come from "several different routes of transmission." Illnesses were reported in North Carolina, South Carolina, Tennessee, and New York. Source: http://www.foodsafetynews.com/2012/05/rare-salmonella-paratyphi-outbreak-grows-as-investigation-continues/

Salmonella sushi outbreak cases jump to 258. Three more states reported illnesses linked to the outbreak of Salmonella infection likely caused by raw sushi tuna imported from India, and the total number of confirmed cases rose to 258, the Centers for Disease Control and Prevention (CDC) reported May 2. The CDC's April 26 update on the Salmonella Bareilly and Salmonella Nchanga infections tied to the product called tuna scrape listed 200 cases from 21 states and Washington, D.C. California, Nebraska, and Tennessee have now reported outbreak-related cases. The 58 new cases include 13 reported by Pennsylvania, 8 by Illinois and New Jersey, 7 by Virginia, 6 by New York, 4 by Maryland, 3 by Massachusetts, 2 by California and Tennessee, and 1 each by Connecticut, Georgia, Nebraska, North Carolina, and Wisconsin. Eleven people infected with the outbreak strain of Salmonella Nchanga were reported from five states: five from New York, two from Georgia and New Jersey, and one from Virginia and Wisconsin. Nearly 59,000 pounds of the frozen yellowfish tuna scrape was recalled by the distributor, Moon Marine Corp. of Cupertino, California. Many of the people sickened reported eating "spicy tuna" sushi before they became ill. Source: http://www.foodsafetynews.com/2012/05/salmonella-sushi-outbreak-cases-jump-to-258/

Hard freeze hits fruit crops. In Canada, Ontario's growing season was over for some farmers before it really began after a killing freeze, London Free Press reported May 1. Apple growers and other fruit farmers took a hit in many areas when temperatures plunged to minus five degrees Celsius and colder April 26 and April 27. Wheat farmers were still waiting to find out how badly their crop was damaged by the weather. Summer-like temperatures early in the spring brought apple blossoms and other crops on early. In some orchards, the freeze left no viable blossoms. The general manager of the Norfolk Fruit Growers' Association said the full extent of the damage to apple and pear crops in the Norfolk area was not yet known. At Heeman's strawberry in London, workers irrigated the crop through the freezing nights when temperatures dipped. The irrigation saved the June crop of berries from any serious damage, although there was some damage to the ever-bearing strawberry crop, said an official. Source:

http://www.lfpress.com/news/london/2012/05/01/19703626.html#/news/london/2012/05/01/pf-19703621.html

Puppy formula part of expanded Diamond Pet Foods recall. Diamond Pet Foods expanded a recall to include Diamond Puppy Formula dry dog food after sampling revealed Salmonella in the product, Food Safety News reported May 2. The recalled Diamond Puppy Formula dry dog food was manufactured at Diamond Pet Foods' plant in Gaston, South Carolina, and distributed in Alabama, Florida, Georgia, Kentucky, Maryland, Michigan, North Carolina, Ohio, Pennsylvania, South Carolina, Tennessee, and Virginia. The product may have been further distributed to additional states through pet food channels. The company said it was working directly with distributors and retailers that carry these products to remove them from the supply chain. Source: http://www.foodsafetynews.com/2012/05/puppy-formula-part-of-expanded-diamond-pet-foods-recall/

(South Carolina) **Irrigation irritation: Recent thefts leave farms' water systems high and dry.** Orangeburg County, South Carolina police officers were looking for a Moncks Corner man after a Eutawville farm's irrigation system was damaged April 24, apparently in an attempt to steal copper wire. Another man was taken into custody April 25 for his part in the damage at the Harvest Court farm. He was charged with malicious injury to personal property of $10,000 or more, grand larceny, and conspiracy. "We are monitoring farms and irrigation systems since these have been the primary targets of copper theft over the past several months," said the sheriff. At about the same time across the county, thieves were plundering another system at Carolina Fresh Farms near Norway. A spokesman for the property said the system suffered about $4,000 in damages. He said over the last 2 years, copper thieves have cost him $60,000 for repairs to 6 irrigation systems. That does not count the crop loss from lack of water. A Clemson extension agent said some farmers are installing cameras and other security systems that alert a farmer through his or her cell phone. Source: http://thetandd.com/news/local/irrigation-irritation-recent-thefts-leave-farms-water-systems-high-and/article_fd41c8dc-8ffd-11e1-816c-0019bb2963f4.html

Diamond Pet Foods expands dry dog food recall. Diamond Pet Foods expanded a recall, announced April 6, for certain batches of Diamond Natural Lamb Meal & Rice dry dog food, to include one production run and four production codes of Chicken Soup for the Pet Lover's Soul Adult Light formula dry dog food. One bag tested positive for Salmonella, and the company said the recall of the four production codes was a precautionary measure, Food Safety News reported April 27. The latest recall is for: Chicken Soup for the Pet Lover's Soul Adult Light Formula dry dog food in 35-pound bags and Chicken Soup for the Pet Lover's Soul Adult Light Formula dry dog food in 6-pound bags. The dog food was distributed in Florida, Kentucky, Massachusetts, Michigan, New York, North Carolina, Ohio, Pennsylvania, South Carolina, and Virginia, and may have been further distributed to other states, through pet food channels. Diamond Pet said it is working directly with distributors and retailers who carry the products to remove them from the supply chain. Source: http://www.foodsafetynews.com/2012/04/diamond-pet-foods-expands-dry-dog-food-recall/

Government Sector (including Schools and Universities)

New 'Unknowns' hacking group hits NASA, Air Force, European Space Agency. A new hacking group calling itself "The Unknowns" published May 1 a list of passwords and documents reportedly belonging to NASA, the European Space Agency, and the U.S. Air Force, among other high-profile government targets. The group's Pastebin post includes names and passwords reportedly belonging to NASA's Glenn Research Center as well as the U.S. Military's Joint Pathology Center, the Thai Royal Navy, Harvard University, Renault, the Jordanian Yellow Pages, and the Ministries of Defense of France and Bahrain. Softpedia reports the hackers also posted screenshots of some of the sites they breached, and that although the post was made public May 1, some of the hacks date back to March. In its message, The Unknowns explained the impetus for their exploits, and warned they could have defaced all of the Web sites. The hackers said they can provide information on how they penetrated the databases, and told the affected organizations to contact them. Source: http://www.securitynewsdaily.com/1804-unknowns-hackers-nasa-air-force.html

(Wisconsin) **Gilman man accused of planning to kill judge, DA, and detective.** A man was taken into custody April 26 after Taylor County, Wisconsin authorities said he planned to a use a bomb to kill a judge, a district attorney, and a detective. He remains behind bars on a $25,000 bond after deputies conducted a search of his home and car and discovered items used to make explosive devices. According to a news release, he had already created one explosive device and planned to detonate it at the Taylor County courthouse. He also stated he knew where the detective lived and planned to follow him home to detonate a bomb there. The Price County district attorney is handling the case. Source: http://www.wsaw.com/news/headlines/Gilman_Man_Accused_of_Planning_to_Kill_Judge_DA_and_Detective_149564285.html?ref=285

(California) **Accused Oikos University shooter pleads not guilty.** The man accused of killing six students and a receptionist in what police described as a revenge mass killing pleaded not guilty April 30 to multiple special circumstances murder charges which make him eligible for the death penalty. The April 2 shooting spree began inside the small university in Oakland, California, when, police said, the suspect walked into a classroom and started shooting students. Police said the suspect was upset the university refused to refund his tuition after he dropped out of school. In interviews with Oakland police, the suspect admitted he went to the college with a .45-caliber handgun and four loaded magazines, that he kidnapped a woman in an office and took her to a classroom, that he shot several people, and that he took the car keys of one of his victims and left in the victim's vehicle, according to the affidavit. Source: http://www.mercurynews.com/bay-area-news/ci_20518435/accused-oikos-university-shooter-pleads-not-guilty

(Connecticut) **Offices remain closed as investigation of Greenwich haz mat incident continues.** Two town hall offices remained off limits to the public and to employees April 30 as local, State, and federal investigators continued their efforts to determine who left a powder-filled

envelope in Greenwich Town Hall in Greenwich, Connecticut, April 26. An official said tests continued to determine the nature of the substance found in an envelope in the ground floor offices of the town's IT and GIS offices. The discovery led to a full-scale response by the Greenwich Fire Department, the Stamford Police Bomb Squad, the Connecticut Department of Emergency and Environmental Protection, and the FBI. The official said the GIS and IT offices remained closed through at least April 30. He also said the incident — which sent one Greenwich police officer to the hospital for evaluation after he was decontaminated at the scene — was prompting a review of security and access to the building. He said police officials will review whether there should be surveillance cameras to monitor who enters the building or a more strict access policy. Crews remained on the scene April 26 for about 5.5 hours. Source: http://greenwich.patch.com/articles/investigation-of-greenwich-haz-mat-incident-continues

Information Technology and Telecommunications

Infected users get legit warning about July 9 'Internet Doomsday'. Two companies, OpenDNS and CloudFlare, have put together a message alert system to help more than a half-million U.S. users who are believed to have the DNSChanger malware on their computers and do not know it, and who may not have heard about it in recent weeks. Infected users will see a message appear on their computer screen. The message says, in part, that the user's Domain Name Server settings suggest "you probably have the DNSChanger malware." Users are then directed to an OpenDNS Web site which has instructions on how to switch DNS to OpenDNS's trusted servers. The message also has a link to the FBI's Web site for more information. Source: http://www.technolog.msnbc.msn.com/technology/technolog/infected-users-get-legit-warning-about-july-9-internet-doomsday-751078

Companies increasingly are dissecting malware in the cloud. Companies increasingly are looking at malware as a source of intelligence to learn more about the threats they face, Dark Reading reports. One of the ways to do this is by using products that provide malware analysis in the cloud. Companies that chance on suspected malware on their networks can upload it to an Internet — or cloud-based — service and get an automated report back detailing how malicious the worm is. These products help firms analyze how malware enters their systems if they do not have the expertise to do it on their own. Companies have historically tapped software or hired security consultants to carry out malware analysis. Of course, organizations concerned that others would gain sensitive information about their system vulnerabilities will have to do the analysis in-house, the report notes. Source: http://www.nextgov.com/cloud-computing/2012/05/companies-increasingly-are-dissecting-malware-cloud/55559/

Service automates boobytrapping of hacked sites. One aspect of hacks seldom examined is the method by which attackers automate the booby-trapping and maintenance of their hijacked sites. This is another aspect of the cybercriminal economy that can be outsourced to third-party services. Often known as "iFramers," such services can simplify the task of managing large numbers of hacked sites that are used to drive traffic to sites that distribute malware and browser exploits. A decent iFramer service will allow customers to verify large lists of file transfer protocol (FTP) credentials used to administer hacked Web sites, scrubbing lists of

invalid credential pairs. The service will then upload the customer's malware and malicious scripts to the hacked site, and check each link to ensure the trap is properly set. Currently, a huge percentage of malware in the wild has the built-in ability to steal FTP credentials from infected PCs. This is possible because those who administer Web sites often use FTP software to upload files and images, and allow those programs to store their FTP passwords. Thus, many modern malware variants will simply search for popular FTP programs on the victim's system and extract any stored credentials. Some services offer a menu of extras to help customers maintain their Web-based minefields. Source: http://krebsonsecurity.com/2012/05/service-automates-boobytrapping-of-hacked-sites/

Trusteer finds new ransomware variant. Ransomware is malware that locks-up computers and demands payment for their release. A common ruse is to pretend the malware is actually a "seizure" by law enforcement agencies. Trusteer recently discovered a new variant. Using the Citadel malware platform — a descendant of the Zeus trojan — the new malware is called Reveton and claims to have come from the U.S. Department of Justice. It locks the computer and displays a warning screen claiming the IP address of the computer was detected accessing child pornography sites. A fine of $100 is payable. It advises how the payment should be made in order to unlock the computer. Source: http://www.infosecurity-magazine.com/view/25490/trusteer-finds-new-ransomware-variant/

Microsoft detects new malware targeting Apple computers. Microsoft detected a new piece of malware targeting Apple OS X computers that exploits a vulnerability in the Office productivity suite patched nearly 3 years ago. The malware is not widespread, a researcher from Microsoft's Malware Protection Center said. However, the malware shows hackers pay attention to people not applying patches when fixes are released, which puts their computers at a higher risk of becoming infected. The security update Microsoft released in June 2009, MS09-027, addressed two vulnerabilities that could be used by an attacker to gain remote control over a machine and run other code. Both vulnerabilities could be exploited with a specially-crafted Word document. The exploit discovered by Microsoft does not work with OS X Lion, but does work with Snow Leopard and prior versions. The researcher said it is likely attackers have knowledge about the computers they are attacking, such as the victim's operating system version and patch levels. The malware delivered by the exploit is written specifically for OS X and is essentially a "backdoor," or a tool that allows for remote control of a computer. Microsoft advised those who use Microsoft Office 2004 or 2008 for Mac or the Open XML File Format Converter for Mac to ensure those products applied the patch. Source: http://www.computerworld.com/s/article/9226777/Microsoft_detects_new_malware_targeting_Apple_computers

Targeted attacks, mobile vulnerabilities on the rise, report states. The findings of the latest "Internet Security Threat Report" from Symantec can be summed up as: "Attacks are rising, but the number of new vulnerabilities is decreasing." This describes the threat landscape in 2011 in which hackers continued to exploit known vulnerabilities through new vectors as enterprises and end users failed to keep up with the flood of security updates from vendors patching their software. "The old vulnerabilities still work," said the manager of Symantec's security

technology and response product group and a contributor to the report. Malware variants are being packaged in attack toolkits that effectively circumvent signature-based defenses. The data in the report is gathered from the company's Global Intelligence Network monitoring activity in more than 200 countries. The total number of vulnerabilities reported in 2011 dropped 20 percent, from a high of 6,253 in 2010 to fewer than 5,000. Over the same time, the number of unique variants of malware identified in the wild increased 41 percent and the number of attacks blocked by Symantec tools jumped 81 percent to 5.5 billion in 2011. The vectors for delivering the malware are shifting, with Web attacks and social engineering through social networks replacing e-mail as the method of choice. This is due in part to successful law enforcement campaigns against command-and-control systems for spam-spewing botnets in 2011, and also because the Web offers a good alternative. Targeted attacks, which have proven to be effective in breaching high-value organizations through carefully crafted social engineering, increased during 2011, from 26 such attacks identified in January of that year to 154 in December. At the same time, the attacks are now targeting smaller organizations and lower-level employees. Source: http://gcn.com/articles/2012/05/01/internet-threat-report-targeted-attacks-mobile-vectors.aspx

Skype investigates tool that reveals users' IP addresses. May 1, Skype said it was investigating a new tool that collects a person's last known IP address, a potential privacy-compromising issue. Instructions posted on Pastebin April 26 show how a person's IP address could be shown without adding the targeted user as a contact by looking at the person's general information and log files. In October 2011, Skype acknowledged a research paper that showed how a Skype user's IP address can be determined without the user knowing. It also demonstrated that more than half the time the IP address could be accurately linked to sharing content using the BitTorrent file-sharing protocol. Skype uses a peer-to-peer system to route its data traffic, which is also encrypted. However, the program's encryption system is proprietary and not been open for scrutiny, which has prompted caution from security experts. Source: http://www.pcworld.com/businesscenter/article/254763/skype_investigates_tool_that_reveals_users_ip_addresses.html

Snow Leopard users most prone to Flashback infection. Of the Macs infected by the Flashback malware, nearly two-thirds are running OS X 10.6, known as Snow Leopard, a Russian antivirus company said April 27. Doctor Web, which earlier in April was the first to report the largest-ever malware attack against Apple Macs, mined data it intercepted from compromised computers to develop its findings. The company, along with other security vendors, has been "sinkholing" select command-and-control domains used by the Flashback botnet — hijacking them before the hackers could use the domains to issue orders or update attack code — to estimate the botnet's size and disrupt its operation. April 27, Doctor Web published an analysis of communications between 95,000 Flashback-infected Macs and the sinkholed domains. Those communication attempts took place April 13. Flashback uses a critical vulnerability in Java to worm its way onto Macs. Although Apple, which continues to maintain Java for its OS X users, patched the bug in early April, it did so 7 weeks after Oracle disclosed the flaw when it shipped Java updates for Windows and Linux. Sixty-three percent of Flashback-infected machines

identified themselves as running OS X 10.6, or Snow Leopard, the newest version of Apple's operating system that comes with Java. Snow Leopard accounted for the largest share of OS X in March, according to metrics company Net Applications, making it the prime target of Flashback. Source: http://www.computerworld.com/s/article/9226696/Snow_Leopard_users_most_prone_to_Flashback_infection?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google

Cybercriminals control Android TigerBot via SMS. At the beginning of April, security researchers found a number of Chinese Android stores were pushing applications that masked a piece of malware called TigerBot (ANDROIDOS_TIGERBOT.EVL). Also known as Spyera, the malicious element was analyzed by Trend Micro experts. They discovered the malware was controlled by its masters via SMS or phone calls, being capable of performing a number of tasks, including call recording and GPS tracking. The list of commands accepted by TigerBot includes DEBUG, CHANGE_IAP, PROCESS_LIST_ADD, PROCESS_LIST_DELETE, ACTIVE, and DEACTIVE.Source: http://news.softpedia.com/news/Cybercriminals-Control-Android-TigerBot-Via-SMS-267066.shtml

Gamex trojan threatens Android users. A new Android trojan that paves the way for the download of other applications has been spotted on third-party Web sites, camouflaged as legitimate file managing, ad blocking, and performance boosting apps. According to Lookout researchers, the Gamex trojan's functionality is split across three components. Once the downloaded app repackaged with the trojan is granted root access by the user, the malware takes advantage of this permission to install another app onto the device, which then functions as a privileged installation service. "A third component communicates with a remote server, downloads apps, and triggers their installation. Gamex also reports the installation of these applications, along with the IMEI and IMSI, to a remote server," researchers explained. "We believe that this information is used to operate and/or report installations to a malicious affiliate app promotion network." Source: http://www.net-security.org/malware_news.php?id=2086&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

Down but not out: Conficker camouflages new Windows infections. Windows PCs infected with Conficker are more likely to be compromised by other malware because the worm masks secondary infections and makes those machines easier to exploit, a security expert found. That is the biggest reason why Conficker, although crippled and seemingly abandoned by its makers, remains a threat and should be eradicated, a senior technologist at Neustar and a cybersecurity adviser to the White House said. Neustar is an information and analytics provider, and one of the corporate members of the Conficker Working Group (CWG), which has been "sinkholing" the Conficker botnet for more than 2 years. The week of April 23, Microsoft said Conficker infected, or tried to infect, 1.7 million Windows PCs in 2011's fourth quarter. Microsoft called on users to strengthen passwords to stymie the malware. Conficker provides the cover the researcher spoke about because of two defensive tactics designed to keep it alive: the worm

disables most antivirus software, including Microsoft's Windows Defender and Security Essentials, and switches off Windows' Automatic Updates, the service used by virtually all Windows users to keep their PCs patched. It also blocks access to security product Web sites — preventing signature updates for antivirus software — and to the Windows Update Web site. Without antivirus software, Conficker-infected systems are unlikely to detect and deflect other malware. If Automatic Updates is disabled, the machine will not receive any new security patches from Microsoft, leaving it open to attack by new threats that exploit those underlying vulnerabilities. Source: http://www.computerworld.com/s/article/9226697/Down_but_not_out_Conficker_camouflages_new_Windows_infections?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_conte

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

(Wisconsin) **Man in custody for placing suspicious envelope in mailbox on east side.** Milwaukee police shut down streets on the lower east side to investigate a suspicious package April 28. Police said a man recorded himself putting a letter he said was laced with anthrax in a mailbox before notifying several media outlets. As it turns out, the letter was a hoax and the man was taken into custody. Knapp Street was closed for nearly 3 hours as police responded to an e-mail they received alerting them to a dangerous package in the area. A video showed the man, with a woman by his side, speaking nonsense, placing a letter addressed to the Wisconsin Department of Workforce Development in the mail on Milwaukee's lower east side. The man then sent an e-mail to various Milwaukee media outlets saying, "There is a letter laced with Anthrax at East Knapp Street," with a link to the video. Source: http://fox6now.com/2012/04/29/milwaukee-police-investigate-suspicious-package-on-knapp-st/

Public Health

FDA says number of new drug shortages down. Health officials said the number of new shortages of crucial drugs used to treat cancer and other illnesses had been halved compared to a year ago, and they attributed the improvement to earlier notice from drugmakers about looming supply issues. There have been 42 newly scarce drugs so far in 2012, compared to 90 in the same period a year ago, the U.S. Food and Drug Administration (FDA) Commissioner said May 3 on the agency's Web site. Efforts to combat shortages escalated in 2011 when 250 medicines were in short supply, up from 56 in 2006. Some doctors have had to postpone care or use second-best drugs or more costly alternatives to compensate for shortages. According to an FDA list, which is updated daily, there are currently about 120 drugs regarded as being in

short supply. Source: http://www.sun-sentinel.com/health/sns-rt-us-fda-shortagesbre8421hg-20120503,0,3898795.story

(Washington) **Wash. uses emergency cash to curb whooping cough.** The governor of Washington opened an emergency fund May 3 to help contain a spreading whooping cough epidemic, and officials urged residents to get vaccinated against the illness that particularly threatens infants. He was making $90,000 in crisis cash available to help strengthen a public awareness campaign about the need for the pertussis vaccination. The State health department is already looking to spend about $200,000 on the effort. The State has also received approval from the federal government to divert some federal cash toward the purchase of 27,000 doses of the whooping cough vaccine. Those will be available for uninsured residents. Washington has already recorded 1,132 cases of whooping cough in 2012 — about 10 times more than the same time last year, according to disease investigators at the health department. The State is recording more than 400 cases of pertussis each month — four times more than the threshold that State officials consider "epidemic" levels — and Washington is on pace for as many as 3,000 cases in 2012. Source: http://www.usatoday.com/news/health/story/2012-05-04/whooping-cough-Washington/54743924/1

FDA formally endorses plague treatment. The U.S. Food and Drug Administration gave formal approval to a new medical countermeasure for preventing and treating infection by plague bacteria, a potential bioterrorism weapon, the Associated Press reported April 29. The regulatory agency said it endorsed the antibiotic Levaquin following trials in which 94 percent of 17 African green monkeys lived through plague infection after receiving the Johnson & Johnson product. Roughly 1,000 to 2,000 global cases of human infection by plague-causing Yersinia pestis bacteria occur annually. Source: http://www.nti.org/gsn/article/fda-formerly-endorses-plague-treatment/

(Illinois) **Hospitals prepare for NATO attack, perform dirty bomb response drills.** April 25, 10 Chicago-area hospitals performed drills simulating a radioactive dirty bomb explosion in preparation for a worst-case scenario during May's NATO summit. An estimated 500 medical professionals and other volunteers donned bulky protective suits, tested radiation detectors, and ministered to about 100 U.S. Navy recruit "victims." The Navy volunteers were posing as victims of a so-called "dirty bomb" that had exploded, leaving them with deadly radioactive cesium on their skin. Doctors and nurses would risk their own lives if they began treating the wounded before they are cleansed of radiation. The dirty bomb scenario was worked out in conjunction with the Secret Service and the DHS. Source: http://www.myfoxchicago.com/dpp/news/metro/suburban-hospitals-prepare-for-nato-attack-perform-dirty-bomb-response-drills-20120426

TRANSPORTATION

(Florida) **Bomb squad safely removes 'suspicious device' from CSX tracks near Jacksonville power plant.** The Jacksonville Sheriff's Office bomb squad safely removed what police described as a "suspicious device" deliberately placed under the rails of CSX tracks in

Jacksonville, Florida, the Jacksonville Times-Union reported May 3. The device was removed about 3 hours after it was discovered by a CSX Transportation Police Department special agent on routine patrol, said a company spokesman. Police would not describe the device, and they did not say whether it was capable of exploding. The FBI confiscated the device. No injuries occurred, and no evacuations were ordered, but firefighters remained on the scene in case they were needed. Authorities handled the discovery of the device with extra care because it was near critical infrastructure, including a JEA power plant. About 10 to 12 freight trains travel the track daily. Source: http://jacksonville.com/news/crime/2012-05-02/story/bomb-squad-safely-removes-suspicious-device-csx-tracks-near-jacksonville#ixzz1toFwaLtQ

(Ohio) **Five arrested in Cleveland plot to blow up bridge.** U.S. authorities arrested five self-described anarchists in the Cleveland, Ohio area for allegedly plotting to blow up a four-lane highway bridge over Cuyahoga Valley National Park, but they had no ties to foreign terrorism, the U.S. Department of Justice said May 1. The group was arrested by the FBI after planting the explosives on the bridge. Three were charged already with conspiracy and attempting to use explosive materials and the other two are expected to be charged later May 1. The FBI said the five arrested were under continuous watch as part of an undercover operation and therefore the public was never in danger. The explosives, supplied by an undercover FBI agent, were inert. The bridge is about 15 miles south of Cleveland in an area popular with hikers and joggers. The group considered a variety of targets for attacks including the Group of 8 leaders meeting in Chicago and the Republican National Convention in Tampa, Florida, according to the FBI affidavit. They also considered igniting smoke grenades off one bridge while they tried to knock large bank signs off the top of big office buildings in downtown Cleveland and even setting off a car bomb outside the Federal Reserve Bank there, the court papers said. Late in April, the group settled on trying to blow up the four-lane Brecksville-Northfield High Level Bridge by placing explosives on some of the columns in hopes of the entire bridge collapsing. The men were expected to appear in federal court. Source: http://www.reuters.com/article/2012/05/01/us-usa-security-cleveland-idUSBRE8400UY20120501

Water and Dams

(Connecticut) **Rising groundwater may flood underground infrastructure of coastal cities.** Pipes, sewers, and basements beneath the coastal city of New Haven, Connecticut, could be flooded by rising groundwater by the end of the century, according to a preliminary study from Yale University and the U.S. Geological Survey (USGS) released May 1. Much of the city's downtown is less than 30 feet above sea level, and advancing waters in the Atlantic could raise groundwater levels as much as 3 feet near the shoreline, the report said, with the potential to "inundate underground infrastructure." Groundwater has risen by as much as 4 feet over the past 100 years in the region, partially because the waters are no longer being used for industrial purposes as they were in the early 1900s. Impacts of another 3- to 4-foot rise in groundwater level is unclear, but many of the city's water mains are below the water table, said the vice president of water quality and outreach for the South Central Connecticut Regional Water Authority. Because groundwater near the coast is salty, it speeds up pipe corrosion. "Rising

groundwater levels are expected to be a chronic problem and will likely be a major issue for all large cities along the coast in the future," said a USGS hydrologist and lead author of the report. Source: http://www.scientificamerican.com/article.cfm?id=rising-groundwater-may-flood-underground-infrastructure-of-coastal-cities

EPA to work with drinking water systems to monitor unregulated contaminants. The U.S. Environmental Protection Agency (EPA) published a list of 28 chemicals and 2 viruses that approximately 6,000 public water systems will monitor from 2013 to 2015 as part of the agency's unregulated contaminant monitoring program, which collects data for contaminants suspected to be present in drinking water, but that do not have health-based standards set under the Safe Drinking Water Act (SDWA). The EPA will spend more than $20 million to support the monitoring. The data collected under the Unregulated Contaminant Monitoring Rule 3 (UCMR 3) will inform the agency about the frequency and levels at which these contaminants are found in drinking water systems across the United States and help determine whether additional protections are needed to ensure safe drinking water. State participation in the monitoring is voluntary. The EPA will fund small drinking water system costs for laboratory analyses, shipping, and quality control. The agency has standards for 91 contaminants in drinking water, and the SDWA requires that the EPA identify up to 30 additional unregulated contaminants for monitoring every 5 years. Source: http://yosemite.epa.gov/opa/admpress.nsf/3881d73f4d4aaa0b85257359003f5348/9725165167f237b1852579f1007176e7!OpenDocument

(Iowa) **Waterworks well damaged by theft seeking copper.** An employee of West Des Moines Waterworks in Iowa, reported April 20 a well house was damaged, the West Des Moines Patch reported April 27. He said the damage occurred when a cable that leads from a communication tower to the well house was cut. Waterworks employees estimated the damage at $1,500. The suspect reportedly cut a 25-foot section of cable. The waterworks employee told a police officer the suspect might have been trying to steal copper. A computer shows information from the well house to the main waterworks facility was interrupted the morning of April 18. Source: http://westdesmoines.patch.com/articles/waterworks-well-damaged-by-theft-seeking-copper

(Connecticut) **Bill sent to gov.** The Connecticut House of Representatives approved legislation that establishes a process to inform the public whenever a sewage spill occurs, the Mystic River Press reported April 30. Sent to the governor for his consideration, the legislation requires the Connecticut Department of Energy and Environmental Protection (DEEP) to post information on unanticipated sewage spills on its Web site beginning in July 2014. The online notice will have details on the spill such as the date, time, volume, duration and steps taken to contain it, as well as public health or environmental concerns and any public safety precautions that should be taken. In July 2013, the DEEP must begin posting information on anticipated sewer overflows resulting from storm events. According to the U.S. Environmental Protection Agency, between 1.8 and 3.5 million Americans become ill annually from contact with recreational waters contaminated by sewage. Currently there is no federal law requiring public notification if a sewage overflow has contaminated a local beach or waterway or entered a community. Source:

http://www.thewesterlysun.com/mysticriverpress/news/rep-urban-bill-sent-to-gov/article_87c05576-8e16-11e1-9070-001a4bcf887a.html

From decade to decade: What's the status of our groundwater quality? There was no change in concentrations of chloride, dissolved solids, or nitrate in groundwater for more than 50 percent of well networks sampled in an analysis released April 30 by the U.S. Geological Survey (USGS) that compared samples from 1988 to 2000 to samples from 2001 to 2010. For those networks that did have a change, seven times more networks saw increases as opposed to decreases. The analysis was done by the USGS National Water Quality Assessment Program (NAWQA) to determine if concentrations of these constituents have increased or decreased significantly from the 1990's to the early 2000's. Though chloride, nitrate, and dissolved solids occur naturally, human activities can cause concentrations to exceed natural levels. At high concentrations, these chemicals can have adverse effects on human and environmental health. The report, "Methods for Evaluating Temporal Groundwater Quality Data and Results of Decadal-Scale Changes in Chloride, Dissolved Solids, and Nitrate Concentrations in Groundwater in the United States, 1988-2010" as well as links to interactive maps showing long-term groundwater trends, can be found on the USGS's Web site. Source: http://www.usgs.gov/newsroom/article.asp?ID=3189#.T565ZdlYtnM

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168